BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 31-601

1 APRIL 1996
Security

★*INDUSTRIAL SECURITY PROGRAM MANAGEMENT*

NOTICE: This publication is available digitally. Contact your Publishing Distribution Office (PDO) for the monthly CD-ROM or access to the bulletin board system. The target date for discontinuing paper publications is December, 1996.

This instruction implements Air Force Policy Directive (AFPD) 31-6, *Industrial Security Program.* It provides guidance for implementing the National Industrial Security Program. Usethis instruction with DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM),* and DoD 5220.22-R, *Industrial Security Regulation,* and DoD 5200.1-R, *Information Security Program Regulation* and changes thereto. See Attachment 1 for a Glossary of References, Abbreviations, Acronyms and Terms, used in this Air Force Instruction (AFI).

SUMMARY OF REVISIONS

This publication has been substantially revised throughout. (*NOTE:* As used in this publication, the term "security review" is not synonymous nor does it negate the "security and policy review" requirement of AFI 35-205, *Air Force Security and Policy Review Program*).

Paragraph

Supersedes: AFI 31-601, 30 December 1993.
OPR: HQ USAF/SPI (Mr. Danny Green)
Certified by: HQ USAF/SP (Brig General Stephen C. Mannell)
Pages: 19/Distribution: F

Paragraph

Page

Chapter 1

GENERAL PROVISIONS AND REQUIREMENTS

1.1. Defining Functional Security Responsibilities.

1.1.1. The senior security official for the Air Force is the Administrative Assistant to the Secretary of the Air Force (SAF/AA), 1720 Air Force Pentagon, Washington DC 20330-1720.

1.1.2. The Assistant for Federal Acquisition Regulation (FAR) System, Deputy Assistant Secretary (Contracting), Assistant Secretary (Acquisition), (HQ USAF/AQC), 1060 Air Force Pentagon, Washington DC 20330-1060, interprets, implements, formulates policy, issues guidance, and supplements FAR requirements.

1.1.2.1. Contracting officers advise, coordinate, and negotiate NISPOM changes with Air Force contractors, to include making appropriate contract modifications and clause revisions, when and where applicable. Existing contracts awarded under terms of the Industrial Security Manual (ISM), should be reviewed on a case-by-case basis and modified as appropriate.

1.1.3. The Air Force Chief of Security Police (HQ USAF/SP), 1340 Air Force Pentagon, Washington DC 20330-1340, formulates, disseminates, interprets policy and provides guidance to Major Commands (MAJCOMs), Field Operating Agencies (FOAs) and Direct Reporting Units (DRUs) on industrial security program requirements.

1.1.4. The Assistant Chief of Staff for Intelligence, Plans, Policy, and Evaluation Directorate, (HQ USAF/INX), 1700 Air Force Pentagon, Washington D.C., 20330-1700, manages the Sensitive Compartmented Information (SCI) security programs under the provisions of Director of Central Intelligence (DCI) Directive (DCID) 1/19, *DCI Security Policy for SCI.*

1.1.5. The Deputy Chief of Staff, Command, Control, Communications & Computers, Director, Architectures, Technologies and Interoperability, (HQ USAF/SCT), 1250 Air Force Pentagon, Washington D.C., 20330-1250, formulates policy and disseminates guidance pertaining to AFPD 33-2, *Information Protection (communications security (COMSEC), computer security (COMPUSEC), and emission security (TEMPEST)).*

1.1.6. The Director of Plans, (HQ USAF/XOX), 1480 Air Force Pentagon, Washington D.C., 20330-1480, formulates policy and disseminates guidance pertaining to AFPD 10-11, *Operations Security (OPSEC),* requirements.

1.1.7. Installation commanders:

- Designate contractor operations requiring access to classified information on their installations as intermittent visitors, visitor groups, or cleared facilities.
- May establish security procedures equivalent to DoD 5220.22-M requirements for contractors operating within the confines of the installation.
- May conduct security reviews of on-base cleared facilities. In these instances, the commander must notify the Defense Investigative Service (DIS) of this decision.
- May designate a servicing security activity, usually a security police unit or equivalent security activity, to perform industrial security program oversight for on-base contractor facilities.

1.1.8. The Secretary of Defense (SECDEF) is the Cognizant Security Agency (CSA) for the Department of Defense (DoD). The SECDEF has designated the Defense Investigative Service (DIS) as the Cognizant Security Office (CSO) for DoD. DIS oversees security for cleared contractor facilities located on Air Force installations at the commander's written request.

1.2. Submitting Inquiries About This AFI.

1.2.1. Submit inquiries and recommendations regarding Air Force Policy Directive (AFPD) 31-6, and/or this instruction through channels to HQ USAF/SPI, 1340 Air Force Pentagon, Washington, D.C., 20330-1340.

1.3. Using References.

1.3.1. Air Force Handbook (AFH) 31-602, provides "how to" and "best business practices" type options and general guidance for establishing and managing an effective industrial security program.

1.4. Defining the Responsibilities of Air Force Servicing Security Activity.

1.4.1 To provide industrial security, the servicing security activity will:

- Conduct security reviews in accordance with National Industrial Security Program Operating Manual (NISPOM), or self-inspections in accordance with DoD 5200.1-R/AFI 31-401, or installation security program requirements, whichever is appropriate for the contractor's operation, as determined by the installation commander.
- Help incorporate appropriate security requirements in classified contract.
- Maintain contract folders on each cleared facility and visitor group that has access to classified information.
- Review draft security classification guides and DD Form 254, for accuracy and appropriateness.
- Implement and oversee the installation industrial security program and coordinate with the offices of primary responsibility (OPRs) that oversee other security disciplines.
- Ensure that personnel report and resolve contractor security violations and compromises promptly.

- Ensure the contractor take prompt corrective actions when a security review of their operation identifies deficiencies that result in an unsatisfactory rating.
- Provide DIS Cognizant Security Office (CSO) a copy of the security review and survey reports and other applicable documentation which pertains to on-base cleared facilities per DoD 5220.22-M, DoD 5220.22-R, AFPD 31-6, and this instruction, if required.
- Work with the contracting office, CSO, and other installation security discipline OPRs to resolve issues pertaining to reciprocity, as applicable to inspections, surveys, audits, security clearances, security reviews, etc. Elevate reciprocity issues to the next higher level of command when they can not be resolved locally.

1.5. Requesting Public Release of Information.

1.5.1. Contracting officers forward contractor requests for public release of information relating to Air Force classified contracts or programs through command public affairs channels. Information requiring Air Force or DoD-level review will be forwarded by the entry-level public affairs office to the Secretary of the Air Force (SAF) Office of Public Affairs (SAF/PA), 1690 Air Force Pentagon, Washington DC 20330-1690. SAF/PA forwards the requests, as required, to the Office of the Assistant Secretary of Defense for Public Affairs (OASD/PA), The Pentagon, Washington DC 20301-1400.

1.5.2. When a contractor reports that classified information has appeared publicly, follow the guidelines in these documents: DoD 5200.1-R; Air Force Policy Directive (AFPD) 31-4, *Information Security Program;* and Air Force Instruction (AFI) 31-401, *Information Security Program Management.*

1.6. Defining Standards for Industrial Security Reviews.

1.6.1 Defining Industrial Security Reviews. The Air Force servicing security activities may conduct security reviews of cleared facilities performing classified work on Air Force installations. Such security reviews, evaluate the contractor's compliance with contract specific-security requirements and pertinent DoD and Air Force security instructions.

1.6.1.1. Visitor group security programs may be evaluated in accordance with DoD 5220.22-M, 5200.1-R/AFI 31-401, or installation security program requirements. The installation commander may prescribe the report format for documenting visitor group self-inspections or installation security program security reviews.

1.6.2. Scheduling Industrial Security Reviews. The servicing security activity conducts security reviews of on-base cleared facilities per DoD 5220.22-M and DoD 5220.22-R. Unless conducting an unannounced security review on a cleared facility, provide contractor activity's management 30 days advanced written notification.

1.6.3. Performing Industrial Security Reviews. The servicing security activity coordinates with other Air Force security discipline OPRs such as; Operations Security (OPSEC), Computer Security (COMPUSEC), Communications Security (COMSEC), etc., to provide specialized expertise when necessary to complete a security review. The security review is complete when all security requirements imposed under the terms of the contract have been evaluated.

1.6.4. Conducting Industrial Security Reviews for Cleared Facilities.

1.6.4.1 When security reviews are conducted for cleared facilities, provide copies of completed DD Forms 696, Industrial Security Inspection Report, or equivalent automated report, with all related correspondence, to the CSO.

1.6.4.2. Facility security clearance (FCL) files must contain all key documentation prescribed by DoD 5220.22-R, and the CSO, to include DD Form 254 and related contract security requirement documents.

1.6.5. Conducting Industrial Security Reviews or Self-Inspections for Visitor Groups.

1.6.5.1. The commander determines the appropriateness and frequency of DoD 5220.22-M, DoD 5200.1-R, or equivalent installation security reviews, or self-inspections for visitor groups.

1.6.5.2. The Air Force activity is responsible for managing and overseeing implementation of DoD 5200.1-R/AFI 31-401, self-inspection requirements, including those Air Force organizations interacting with visitor groups who are authorized to operate under AFI 31-401 requirements.

1.6.5.3. The servicing security activity establish and maintain files for each visitor group. The files should contain a copy of the visitor's group security agreement, a current listing of the key management officials, the current DD Form 254, copies of self-inspections orequivalent installation security program reportsand other pertinent correspondence.

1.6.5.4. Do not furnish the CSO copies of visitor group self-inspection reports or related correspondence.

1.6.6. Post-Industrial Security Review Requirements for Cleared Facilities.

1.6.6.1. Within 10 days after completing a industrial security review, the servicing security activity sends a letter to the senior management official of the cleared facility:

- Confirming the contractor's security status as discussed during the exit interview.
- Listing any deficiencies requiring corrective action.
- Within 30 days, request written confirmation on the status of any open major discrepancy (condition which resulted in or could reasonably be expected to result in the loss or compromise of classified information).
- The servicing security activity may extend the time for corrective action if required changes are

significant and the contractor is making a conscientious effort to resolve problems expeditiously.

1.6.7. For visitor groups, the servicing security activity should brief key Air Force activity and visitor group managers on the status of the contractor's security program efforts. Provide both parties a copy of any related assessment, survey or staff assistance visit (SAV) reports, if applicable.

1.6.7.1. For visitor groups, Air Force commanders notify the contractor's home office facility (HOF), in writing, through the contracting office of major security program deficiencies or non-compliance with the terms of the visitor group security agreement.

1.6.8. Defining Requirements for Reporting and Maintaining Records.

1.6.8.1. The servicing security activity will:

- Keep files for each cleared facility and visitor group.
- Document security reviews for cleared facility as required by the DoD 5220.22-M, DoD 5220.22-R, and CSO guidance. Keep copies of completed security review reports with pre-security review letter and complete post-review correspondence, for 2 years from the date of the most recent security review.
- Maintain copies of visitor group self-inspection reports for 1 year from date of the most recent self-inspection.

1.7. Defining Unsatisfactory Industrial Security Reviews.

1.7.1. The servicing security activity assigns cleared facilities an unsatisfactorysecurity review rating:

- To a cleared facility if it fails to satisfactorily perform its contractual security responsibilities.
- When major failures in the contractor's security program have resulted in or could reasonably be expected to result in the loss or compromise of classified information.
- When the contractor is clearly responsible for the security problems cited during a security review.

1.7.2. The Servicing security activity coordinates with the CSO and contracting officer when assigning an unsatisfactory security review rating for an on-base cleared facility.

1.7.3. The home office facility (HOF) for the cleared facility is ultimately responsible for meeting contract security requirements. When assigning an unsatisfactory security review rating, the servicing security activity notifies the HOF immediately through the contracting office and requests prompt and complete corrective action. If the HOF fails to take corrective action, its security clearance may be affected. The servicing security activity should notify the HOF's CSO if problems continue.

1.7.4. Do not assign a rating to "self-inspections" conducted by visitor group operating under the provisions of DoD 5200.1-R/AFI 31-401.

1.8. Invalidating the Facility Security Clearance (FCL) .

1.8.1. The CSO notifies contracting officers in writing when the facility security clearance (FCL) of a contractor under their jurisdiction is invalidated.

1.8.2. A contractor who fails to correct security deficiencies that subsequently results in a FCL invalidation may lose its FCL.

1.8.3. Although most contractors resolve invalidations promptly, contractors with foreign owned, controlled, or influence (FOCI) invalidations may have to wait for many months. Where FOCI is evident, the cleared facility may remain invalidated for more than a year while methods to resolve the FOCI are considered, approved, and implemented. The FCL is invalidated while DIS negotiates voting trusts, proxy agreements, or special agreement with foreign interests.

1.9. Adverse Information and Suspicious Contacts Reporting Requirements for Visitor Groups.

1.9.1. Visitor groups operating under DoD 5200.1-R/AFI 31-401 or installation security program may satisfy NISPOM adverse information and suspicious contacts reporting requirements by submitting the appropriate report or information as required by the NISPOM to the servicing security activity. Incorporate the specific terms of this reporting requirement into the Visitor Group Security Agreement (VGSA), if applicable.

1.9.1.1. Upon receipt of information submitted per paragraph 1.9.1., the servicing security activity will forward the report to the visitor group's HOF. Any subsequent or additional reporting required by the NISPOM to other federal agencies, i.e., CSA, CSO, FBI, etc., is thereafter the responsibility of the HOF.

1.9.1.2. The servicing security activity will retain a copy of the adverse information or suspicious contracts report in the visitor group's files for 2 years.

1.9.1.3. The servicing security activity is responsible for notifying other AF activities, i.e., contracting office, OSI, etc., when appropriate.

1.10. Reporting Security Violations.

1.10.1. Cleared facilities report the loss, compromise, suspected compromise or other security violations to the CSO pursuant to DoD 5220.22-M. On-base contractor facilities may also report such instances through the servicing security activity, which reports the information to the CSO. Written agreements may direct visitor groups to report such incidents or information in accordance with DoD 5200.1-R/AFI 31-401 to the servicing security activity. The CSO and the servicing security activity report significant (resulting in actual loss or compromise) contractor security violations and compromises of classified to the contracting officer.

1.10.2. Reporting Espionage, Sabotage, and Subversive Activities.

1.10.2.1. The servicing security activity reports espionage, sabotage, subversive activities, deliberate compromises of classified information, and leaks of classified information to the media, involving cleared facilities or visitor groups located on Air Force installations to the servicing Air Force Office of Special Investigations (AFOSI). AFOSI coordinates with the Federal Bureau of Investigations (FBI), as appropriate. The servicing security activity sends a report via secure communications (STU III or classified fax) with an information copy to each of the following activities:

- The CSO
- The OPR
- HQ USAF/SPI
- HQ USAF/PA
- The MAJCOM headquarters and the Subordinate headquarters, if appropriate.

1.10.2.2. Such a report should:

- Identify the cleared facility or visitor group involved. Identify the person(s) involved, including the full name, date and place of birth, Social Security number, local address, present location, position with the contractor, security clearance (including past or present participation in any special access programs (SAPs)), and a description on any plans or action and any recommendations to suspend or revoke the individual's personnel security clearance (PCL).
- Establish the known circumstances of the incident, including the classified material involved; any subsequent activities or circumstances (including whether and which news media know about the incident); and culpable individuals, where known.
- Document when (time and date) the servicing security activity reported the incident to the AFOSI or when the CSO reported the incident to the FBI.

Include a copy of any investigative report.

- Identify any changes in contractor procedures necessitated by the incident and any recommendations for change in the security program which might prevent similar future violations.

1.10.3. The reporting requirement in paragraph 1.10.2. is exempt from licensing with a report control symbol (RCS) IAW paragraph 2.11.1. of AFI 37-124, *The Information Collections and Reports Management Program.*

1.11. Reporting Loss, Compromise, and Possible Compromise

1.11.1. The installation commander follows the instructions and performs actions directed by DoD 5220.22-R to report the loss, compromise, or possible compromise of classified information for on-base contractor operations for which the Air Force has retained security oversight.

1.11.2. Contracting officers who learn of contractor loss, compromise, or possible compromise of Air Force classified information immediately notify the servicing security activity and the Air Force functional office that has responsibility for the compromised information.

1.11.3. The commander of the affected organization or original classification authority is responsible for damage assessment and corrective actions.

1.11.4. Notify the Air Force commander, CSO, and/or the contractor of decisions to declassify, downgrade, or retain classification of the affected information. Do not give copies of damage assessment reports to the CSO or cleared facility operations.

1.11.5. Unless CSO assistance is needed, do not notify the CSO of the results of a classification review or action begun or taken to mitigate damage to national security.

1.11.6. Unless otherwise directed, handle correspondence associated with such incidents directly between the CSO and/or servicing security activity and the affected Air Force activity.

1.11.7. The servicing security activity provides copies of investigation and inquiry reports and related correspondence to the appropriate CSO and HOF that has jurisdiction over the visitor group.

Chapter 2

SECURITY CLEARANCES

2.1. Defining Facility Security Clearances (FCLs).

2.1.1. Sponsoring FCLs. DIS CSO is the authorizing agent for FCL sponsorship. DIS CSO establishes and maintains all FCLs within the National Industrial Security Program (NISP). Also see DoD 5220.22-M, DoD 5220.22-R, AFPD 31-5, *Personnel Security,* and AFI 31-501, *Personnel Security Program Management.*

- To request FCL sponsorship, write to the CSO with oversight for the sponsored facility. DIS CSO establishes and maintains all FCLs within the National Industrial Security Program.
- Give the full name for the sponsored facility, its physical and mailing address, telephone number, and a specific point of contact at the facility, when known. Give the full name, job title, and direct-dial telephone number of the Air Force sponsor.
- Establishing final FCLs through DIS CSO may take several months. When circumstances do not permit such delays, sponsors may request an interim FCL through DIS CSO.

2.1.2. Sponsoring Interim FCL. DIS CSO automatically processes all requests for Confidential and Secret FCLs for interim clearances when possible. However, Air Force sponsorship of interim Top Secret FCLs must be justified on a case-specific basis in accordance with DoD 5220.22-R. To request a Top Secret interim FCL:

- Contracting officers prepare and route sponsorships through command channels to the MAJCOM, FOA, or DRU commander for approval. Each request must include these items:
- An explanation of why an interim Top Secret FCL would prevent a crucial delay in the award or performance of a classified contract.
- A list giving the legal name of the facility seeking sponsorship, its complete street address, and the names and positions of people who are applying for interim Top Secret access authorization.
- The address of the authorizing DIS.

2.1.3. Establishing FCLs. The office of record for the FCL, calledthe DIS CSO, establishes the FCL**.**

- The servicing security activity with oversight responsibility for an FCL on the installation conducts required security reviews of the FCL's operation and assists the CSO, as necessary.
- The servicing security activity also conducts FCL surveys and administrative inquiries of the FCL as requested by the CSO and ensures contractor compliance with DoD 5220.22-M
- Complete the survey by using the DD Form 374, **Facility Security Clearance Survey Data Sheet-,**when conducting survey for a on-base cleared facility and give a copy to the CSO. These forms are stocked and issued by DIS, 1900 Half St., SW, Washington, D.C., 20330-1700.

2.2. Advising About Contractors with Foreign Ownership, Control, or Influence (FOCI).

2.2.1. The CSO tells contracting officers if a contractor performing on a classified contract has FOCI. Such influence might jeopardize the security of classified information held by the contractor.

2.2.2. To resolve a FOCI problem, the CSO may establish a facility clearance that limits the level and type of classified information to which a FOCI contractor has access. Such restrictions might affect ongoing, pending, and future classified contracts with the contractor. Contracting officers should discuss this impact with the servicing security activity and command foreign disclosure authorities.

2.2.3. Contracting officer should consider sponsoring National Interest Determination (NID) when a FOCI contractor's product or services are crucial or the sole available source, or when contract cancellation would cause unacceptable delays for mission-essential weapons systems in the field or for support organizations.

2.2.4. Forward requests for NIDs related to SAP performance through the appropriate SAP and command channels to the Deputy for Security and Investigative Programs, Office of the Administrative Assistant (SAF/AAZ), 1720 Air Force Pentagon, Washington, D.C. 20330-1720 for approval. Forward requests for all other NIDs through command channels to HQ USAF/SPI for endorsement by SAF/AAZ. SAF/AA approves NIDs with the Air Force and forwards them for final approval to the Director, Defense Security Programs, Office of the Deputy Assistant Secretary of Defense for Counterintelligence and Security Countermeasures, Office of the Assistant Secretary of Defense for Command, Control, Communication, and Intelligence, Pentagon, Washington, D.C. 20301-3040.

2.3. Obtaining Personnel Security Clearances (PCLs) for Contractor Personnel.

2.3.1. Defense Industrial Security Clearance Office (DISCO), an operational element of DIS, grants and maintains contractor PCLs. DISCO also terminates contractor PCLs when the contractor no longer needs them or when a contractor employee terminates.

Administrative termination of a PCL carries no adverse implications regarding the employee or the contractor.

2.3.2. The Directorate for Industrial Security Clearance Review, DoD Office of General Counsel, may suspend or revoke contractor PCLs following due process.

2.3.3. DIS automatically processes all requests for Confidential or Secret PCLs for interim clearances where possible.

2.3.4. When a contractor employee who is not cleared for access to Top Secret information needs such access to perform on an Air Force classified contract, the employing contractor may sponsor the individual for an interim Top Secret PCL.

- The contractor should send requests through contracting channels to the contracting officer, System Project Office (SPO), System Manager (SM), or Program Manager (PM).
- The contractor's request should document clearly why the individual needs an interim PCL, why contract requirements may not be satisfied with another individual more suitably cleared, and what the potential adverse impact would be on contract performance if an interim PCL were not granted. The contracting officer will deny contractor requests that do not meet these criteria.

2.3.5. The contracting officer routes the appropriate contractor's request for interim Top Secret PCLs to the MAJCOM, FOA, or DRU commander for approval.

2.3.6. The contracting officer sends favorably endorsed requests to the contractor, who then includes the endorsement in the personnel security questionnaire package for transmission to DISCO for action. The contracting officer promptly returns denied requests.

Chapter 3

SECURITY TRAINING AND BRIEFINGS

3.1. Security Awareness Training for Contractors.

3.1.1. Classified contracts may stipulate (statement of work, VGSA, etc.) contractor compliance with and participation in pertinent Air Force, command and installation security programs.

3.1.2. When specified in the visitor group security agreement, the base information security training program will satisfy NISPOM security training requirements for visitor groups, including required security briefings or debriefings. Coordinate this provision with other Air Force security discipline OPRs, as necessary.

3.1.3. When designated, the servicing security activity provides the initial facility security officer (FSO) briefing for cleared facility operations in accordance with CSO guidance.

3.1.4. Air Force security managers may provide security support for visitor groups.

3.1.5. Visitor groups operating under DoD 5200.1-R/AFI 31-401 may attend Air Force conducted security education and awareness training. If this training meets and satisfies NISPOM requirements, no additional contractor administered training is required.

3.1.6. If specified in the VGSA, contractor personnel operating under DoD 5200.1-R/AFI 31-401 may be appointed alternate or office security managers duties.

Chapter 4

CLASSIFICATION AND MARKING

4.1. Defining DD Form 254 and Visitor Group Security Agreement (VGSA).

4.1.1. The program and contracting offices implement NISPOM requirements through contract documents. Only contracting offices can modify contracts or negotiate changes.

4.1.2. When a contractor needs access to classified information, prepare a

DD Form 254. The contractor should use the security requirements in this form to accurately estimate the cost of security measures. More detailed security requirements are laid out in the statement of work, annexes to the DD Forms 254, or VGSA.

4.2. Issuing Security Classification Guidance.

4.2.1. Program or project offices prepare DD Form 254. Program Managers (PMs) develop security classification guidance at the program level. Contracting officers review and coordinates the DD Form 254 for each classified procurement with the appropriate security discipline OPRs. This action ensures that appropriate and approved security classification guidance has been incorporated into contract and provided to the contractor.

4.2.2. Procuring Contracting Officers (PCOs) or their designated representatives, including Administrative Contracting Officers (ACOs), distribute DD Form 254.

4.2.3. When completing DD Form 254s, develop a draft by consulting the servicing security activity, and other installation security discipline OPRs affected under the terms of the DD Form 254. Indicate such coordination in the remarks section (Block 13) DD Form 254, or separate attachment. When SAPs are involved, coordinate draft DD Form 254 with the office responsible for SAP security oversight. Keep DD Forms 254 for SAPs unclassified when possible.

4.3. Sending Copies of Required Forms.

4.3.1. When DIS is relieved of security oversight responsibility for cleared facilities performing on SCI or SAP programs, furnish Headquarters DIS, 1340 Braddock Place, Alexandria VA 22314-1651, a copy of the DD Form 254.

4.3.2. When a contractor must perform on Air Force installations, specify all performance locations, if known, on the DD Form 254. Coordinate DD Form 254 requirements with performance location servicing security activity, when contract is performed elsewhere. and provide copies (draft, revised, final, etc.) of the DD Form 254 to that activity.

4.3.3. For coordination purposes, route DD Form 254 to all Air Force security discipline OPR and/or other Air Force agencies lending expertise to the servicing security activity that oversees contract security requirements.

4.4. Reviewing and Certifying DD Form 254.

4.4.1 The servicing security activity reviews the security classification guidance in the DD Form 254 to ensure that is accurate, approved, and appropriate.

4.4.2. The program manager normally certifies DD Form 254. The contracting officer may also certify it.

Chapter 5

SAFEGUARDING CLASSIFIED INFORMATION

5.1. Defining Security Requirements for Visitor Groups.

5.1.1. Visitor groups operating in accordance with DoD 5200.1-R/AFI 31-401 or an installation security program may handle, generate, process, and store classified information dually per the Air Force activity's security program procedures and requirements.

5.1.2. When a visitor group is permitted to operate under DoD 5200.1-R/AFI 31-401 requirements, the Air Force activity must limit the visitor group's access to "need-to-know" contract-specific performance information only.

5.1.3. Program and project offices must stipulate the specific DoD 5200.1-R/AFI 31-401 or installation security program requirements that are applicable in the VGSA or an appropriate contracting document. Mandated security requirements not addressed or covered in the VGSA or other contracting documents must be implemented by the visitor group in accordance with the NISPOM.

5.1.4. The VGSA must clearly reflect that the Air Force is accountable for and controls all classified information. Visitor groups operating under the provisions of DoD 5200.1-R/AFI 31-401 are prohibited from establishing separate classified information controls. See sample VGSA in AFH 31-602.

Chapter 6

VISITS AND MEETINGS

6.1. Visitor Groups.
6.1.1. The installation commander establishes visitor groups.

6.2. Air Force Visits to Contractor Facilities.
6.2.1. Air Force personnel who require access to classified information while visiting contractor facilities must comply with the provisions of DoD 5200.1-R and DoD 5220.22-M.

6.3. Contractor Visits to Air Force Installations.
6.3.1 DoD contractors located on or visiting Air Force installations in support of a classified contract must comply with DoD 5220.22-M, Chapter 6, Section 1, visit requirements.

6.3.2. Installation commanders establish procedures for processing and coordinating incoming contractor visit requests.

6.3.3. Identify specific procedures for receiving, processing, and handling in-coming visitor group visit request in the VGSA and AF activity's information security program operating instruction (OI). Whenever possible, these incoming request should be directed to and maintained on file by the AF activity's unit security manager**.**

Chapter 7

SUBCONTRACTING

7.1. Defining Prime Contractor's Responsibilities. 7.1.1. Include responsibility for ensuring subcontractor compliance with DoD 5220.22-M, DoD 5200.1-R/AFI 31-401, or installation information security program requirements in the prime contractor's VGSA or enter into a separate VGSA with the subcontractor.

Chapter 8

AUTOMATED INFORMATION SYSTEM (AIS) SECURITY

8.1. Defining Guidance for AIS Accreditation.

8.1.1. When industrial security program oversight is retained by Air Force for on-base cleared facilities, the contracting office coordinates AIS accreditation, COMSEC, and TEMPEST requirements with the responsible installation security discipline OPRs and DIS through the servicing security activity.

8.1.2. Visitor groups may use approved Air Force AISs and/or networks to process classified information.

Chapter 9

SPECIAL REQUIREMENTS

9.1. Defining Guidance for Special Access Programs and Sensitive Compartmented Information (SCI).

9.1.1. For a carve-out contract, the Special Access Program (SAP) program manager assigns an Air Force element to perform security reviews and oversight. (Also see DoD 5220.22M-Sup 1, *National Industrial Security Program Operating Manual (NISPOM) Supplement*, and AFI 16-701, *Special Access Programs.)*

9.1.2. Program managers for Air Force SAP and SCI programs may relieve the designated CSO and servicing security activity from security review and oversight responsibility for cleared facilities and/or visitor groups. Such relief normally will be limited to specific SAP and SCI information.

Chapter 10

INTERNATIONAL SECURITY REQUIREMENTS

10.1. Defining Procedures for Contractor Operations Overseas.
10.1.1. DoD policy does not allow FCLs for contractor operations located outside the US, Puerto Rico, or a United States possession or trust territory. Treat contractor operations supporting the Air Force overseas as visitor groups or intermittent visitors.

10.2. Giving Foreign Visitors Access to Information.
10.2.1. Foreign persons occasionally request access to classified or unclassified information for an Air Force contract while visiting United States cleared facilities. Advise the visitor to process the request through the sponsoring foreign government, which submits the request to the Air Force Foreign Disclosure Office, SAF/IAW, 1010 Air Force Pentagon, Washington DC 20330-1010.

10.3. Processing Requests for Technology Transfer.
10.3.1. United States national disclosure policy permits cleared United States facilities to enter into direct commercial arrangements involving the disclosure of classified information to foreign companies. Such arrangements are subject to specific circumstances, which may include public law, regulations, bilateral security agreements executed between the United States Government and certain allied and friendly foreign governments, and program specific memoranda of understanding. See DoD 5220.22-M, Chapter 10, Section I.

10.4. Releasing Classified Information to a Foreign Interest.
10.4.1. Contractors request permission to disclose classified information to a foreign interest through command channels to SAF/IAW. If SAF/IAW authorizes disclosure, transmit the classified material through government-to-government channels.

10.5. Foreign Visits. Foreign visits to on-base contractor locations must be coordinated through normal Air Force channels, at least 10 days in advance.

Chapter 11

MISCELLANEOUS INFORMATION AND GUIDANCE

11.1. Security Plans, Procedures, Operating Instructions and Training Material.

11.1.1. Contractors may use existing Air Force security program related plans (Operations Security, Program Protection, Automated Information Systems, etc.), procedures, operating instructions (OIs), and educational/training materials that meet the intent of and satisfy NISPOM requirements. Coordinate with other security discipline OPRs, when applicable, and incorporate authority for their usage in the VGSA or other appropriate contracting documents.

11.2. Defining Applicability of Other Security Program Requirements.

11.2.1. Coordinate security requirements, not stipulated in the NISPOM, with the responsible security discipline OPR and DIS, if applicable.

11.2.2. Security specialists representing related security functions may accompany the servicing security activity or CSO representative during security reviews or when requested.

11.3. Forms Prescribed. DD Form 254, **DoD Contract Security Classification,** DD Form 374, **DoD Facility Security Clearance Survey Data Sheet, and** DD Form 696, **Industrial Security Inspection Report.**

STEPHEN C. MANNELL, Brig General, USAF
Chief of Security Police

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

References

DoD 5200.1-R, *Information Security Program Regulation*
DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*
DoD 5220.22-M-Sup 1, *National Industrial Security Operating Manual Supplement (NISPOMSUP)*
DoD 5220.22-R, *Industrial Security Regulation*
AFPD 10-11, *Operations Security*
AFPD 31-4, *Information Security*
AFPD 31-5, *Personnel Security*
AFPD 31-6, *Industrial Security*
AFPD 33-2, *Information Protection*
AFI 16-701, *Special Access Programs*
AFI 31-401, *Information Security Program Management*
AFI 31-501, *Personnel Security Program Management*
AFI 31-601, *Industrial Security Program Management*
AFI 35-205, *Air Force Security and Policy Review Program*
AFI 37-124, *The Information Collections and Reports Management Program*
AFH 31-502, *Personnel Security Program Handbook*
AFH 31-602, *Industrial Security Program Handbook*
DCID 1/19, *DCI Security Policy for SCI*

Abbreviations and Acronyms

ACO−Administrative Contracting Officer
AFH−Air Force Handbook
AFI−Air Force Instruction
AFOSI−Air Force Office of Special Investigations
AFPD−Air Force Policy Directive
AIS−Automated Information System
C4−Command, Control, Communications, and Computers
COMSEC−Communications Security
CSO−Cognizant Security Office
DD−Department of Defense
DIS−Defense Investigative Service
DISCO−Defense Industrial Security Clearance Office
DoD−Department of Defense
DRU−Direct Reporting Unit
FAR−Federal Acquisition Regulation
FBI−Federal Bureau of Investigations
FCL−Facility Security Clearance
FOA−Field Operating Agency
FOCI−Foreign Owned, Controlled, or Influenced
HOF−Home Office Facility
MAJCOM−Major Command
NATO−North Atlantic Treaty Organization
NID−National Interest Determination
OPR−Office of Primary Responsibility
OPSEC−Operations Security
PCL−Personnel Security Clearance
PCO−Procuring Contracting Officer
PM−Program Manager
RFP−Request for Proposal
RFQ−Request for Quote
SAF−Secretary of the Air Force
SAP−Special Access Program

SAV−Staff Assistance Visit
SCI−Sensitive Compartmented Information
SM−System Manager
SPO−System Project Office
VGSA−Visitor Group Security Agreement

Terms

Carve-out Contract— A carve-out contract is a classified contract for an approved SAP in which the DIS has partial or no oversight or security review responsibility. The Air Force SAP manager for a carve-out contract designates an Air Force activity to perform these functions.
Cleared Facility— A non-government owned or operated industrial, educational, commercial, or other facility for which DoD has made an administrative determination (from a security viewpoint) that the entity is eligibility for access to classified information of a certain category (Confidential, Secret, or Top Secret).
Cognizant Security Office— The designated Department of Defense (DoD) agency responsible for industrial security program administration. The Secretary of Defense (SECDEF) has designated the Defense Investigative Service (DIS) to perform this function. The Director of DIS, has further delegated this responsibility downward within the agency. DIS Regional Directors provide industrial security administration for DoD contractor facilities located within their respective geographical area. The exception being, installation DoD contractors designated as "visitor Group" for which the SSA have these responsibilities. When used, the language "Cognizant Security Office" (CSO), always refers to DIS or an entity thereof.
Interim Facility Security Clearances (Interim FCL)— Interim FCL are temporary, limited company security clearances established by the DIS CSO. It does not permit access to Restricted data, COMSEC, North Atlantic Treaty Organization (NATO), SCI, SAP, or Arms Control and Disarmament Agency classified Information. However, if an interim Top Secret PCL is issued, the contractor may access such information at the level of Secret and Confidential. Interim FCLs may not be appropriate for all contractual needs and are not available for all sponsored companies.
Installation— An installation is an area in which the Air Force holds a real property interest or real property over which the Air Force has jurisdiction by agreement with a foreign government or by right of occupation. The term installation also includes all auxiliary off-base or detached installations under the jurisdiction of the commander of the primary installation.
Intermittent Visitors— Contractor employees visiting an Air Force installation for brief periods of time on a scheduled or on call basis to perform contractual duties that require access to classified information. An intermittent visitor's presence on an installation usually does not exceed 90 consecutive days.
Invalidation— A temporary condition at a cleared facility caused by changed conditions or performance under which the facility may no longer be eligible for an FCL unless the facility promptly initiates appropriate corrective actions.
Major Discrepancy— A condition which resulted in or could reasonably be expected to result in the loss or compromise of classified information.
Reciprocity— A reciprocal condition, relationship, mutual or cooperative agreement, between two or more agencies, components, or departments agreeing to recognize and accept the efforts (requirements, procedures, actions, etc.) of the other in exchange for the same compensation.
Servicing Security Activity— This activity implements and oversees the industrial security program for an installation and designated on-base contractors. The installation commander designates the servicing security activity.
Visitor Groups— A contractor operation on an Air Force installation that requires access to classified information. It operates under the direct control of the Air Force. It differs from a cleared facility by its close interaction and/or working relationship with an Air Force organization. Normally, the visitor group operation is integrated into and directly supports the organization's mission. However, unlike a cleared facility, the visitor group does not have the capability to handle, process, or store classified information independent of the Air Force activity. It differs from an intermittent visitor primarily because of its long-term presence on an installation.
Visitor Group Security Agreement— A documented and legally binding contractual agreement between an Air Force activity and a DoD contractor whereby the contractor commits to rendering or performing specific security services for compensation. The VGSA attest to and certifies the existence of such an agreement, including applicable changes and amendments, attachments, supplements and exhibits.